REMARKS

Applicants appreciate the thorough examination of the present application as reflected in the Final Official Action mailed April 21, 2005 (hereinafter "Official Action"). Applicants particularly appreciate that the Examiner has withdrawn the rejection of Claims 8-10, 36-38 and 64-66. In addition, Applicants request that the Examiner reconsider the rejection of the remaining claims for the reasons discussed below. Applicants request entry of the present Amendment as Applicants submit that it raises no new issues. Applicants submit that the present application is in condition for allowance for at least the reasons discussed below.

I. Amendments to the Specification

Applicants have amended the specification to correct typographical errors including incorrect figure references. No new matter has been introduced. In particular, the figure reference in the first sentence of the first full paragraph of page 26 should refer to Figure 9 instead of Figure 8, since the discussion in that paragraph continues the discussion of the retrieval of an encrypted file by a client of a trusted third party. Specifically, the discussion relates to the operation of blocks 704 - 710 which are illustrated in Figure 9, not Figure 8.

II. Applicants Request Reconsideration Of The Claim Rejections

Claims 1-7, 29-35 and 57-63 stand rejected under 35 U.S.C. § 103 as obvious in light of United States Patent No. 5,495,533 to Linehan (hereinafter "Linehan") and United States Patent No. 6,023,506 to Ote (hereinafter "Ote"). Official Action, p. 4. Claims 11-17, 39-45 and 67-73 stand rejected under 35 U.S.C. § 103 as obvious in light of Linehan, Ote and United States Patent No. 5,734,819 to Lewis (hereinafter "Lewis"). Official Action, p. 5. Claims 18-20, 46-48 and 74-76 stand rejected under 35 U.S.C. § 103 as obvious in light of Linehan, Ote and United States Patent No. 5,805,712 to Davis (hereinafter "Davis"). Official Action, p. 7. Claims 21-28, 49-56 and 77-84 stand rejected under 35 U.S.C. § 103 as obvious in light of Linehan, Ote, Davis and Lewis. Official Action, p. 8. Applicants will address each of the rejections separately below.

A. Claims 1-7, 29-35 and 57-63

Claims 1-7, 29-35 and 57-63 stand rejected under 35 U.S.C. § 103 based on the combination of Linehan and Ote. As noted in prior communications, the mere fact that references can be combined or modified does not render the resultant combination obvious unless the prior art also suggests the desirability of the combination. M.P.E.P. §2143.01, citing *In re Mills*, 916 F.2d 680, 16 U.S.P.Q.2d 1430 (Fed. Cir. 1990). Moreover, to support combining or modifying references, there must be **particular** evidence from the prior art as to the reason the skilled artisan, with no knowledge of the claimed invention, would have selected these components for combination in the manner claimed. *In re Kotzab*, 55 U.S.P.Q.2d 1313, 1317 (Fed. Cir. 2000). There is no such teaching or suggestion in the cited portions of Ote or Linehan. In fact, as will be discussed below, Linehan teaches away from combination with Ote to produce the invention as claimed in Claims 1-7, 29-35 and 57-63. In order to understand why this is the case, the operation of the Linehan system will be discussed briefly.

1. Operation of the Linehan System

Linehan describes two systems for encryption key management: a basic system described in col. 7, line 30 to col. 8, line 45 thereof, and an enhanced system described in col. 8, line 46 to col. 10, line 45 thereof.

In both the basic and enhanced systems of Linehan, a Personal Key Server assists in the process of encrypting and decrypting files. See e.g., Linehan, col. 4, line 61 - col. 5, line 16. The Personal Key Server communicates with Personal Key Client applications that reside on user computers. See Linehan, col. 6, lines 17-38. Multiple Personal Key Clients may access the Personal Key Server remotely through a network. See Linehan, col. 6, lines 33-37. Files are encrypted and decrypted using file encryption keys that may be generated at the Personal Key Client or the Personal Key Server. See Linehan, col. 7, lines 48-53; col. 8, lines 37-41. However, file encryption and decryption is performed at the Personal Key Client, not at the Personal Key Server. See Linehan, col. 7, lines 30-33; col. 9, lines 26-29.

In the basic system, the file encryption keys are stored at the Personal Key Server and provided to Personal Key Clients upon request over a secure link. See Linehan, col. 7, lines 33-34; lines 60-64. In the basic system, the Personal Key Server stores each file encryption key together with the file name and the file creation date. See Linehan, col. 7, lines 39-45. Authentication is provided by an authentication server using a ticket-based authentication system such as Kerberos. See Linehan, col. 7, lines 34-36. When a user needs to decrypt a file, the Personal Key Client sends the file name and file creation date to the Personal Key Server. See Linehan, col. 7, lines 54-57. Once the request has been authenticated, the Personal Key Server retrieves the file encryption key associated with the file and sends it to the Personal Key Client, which uses the file encryption key to decrypt the file. See Linehan, col. 7, lines 54-64. Session encryption is used to protect the file encryption key during transmission to the Personal Key Client. See Linehan, col. 8, lines 17-19. Thus, in the basic system, the Personal Key Server stores a separate record for each encrypted file, which may require excessively large and complex database. See Linehan, col. 11, lines 48-57.

In the enhanced system, rather than storing the file encryption keys, the Personal Key Server manages a database of randomly generated control keys, which are used to encrypt the file encryption keys of multiple users' files. Control keys are generated by and kept entirely within the Personal Key Server. See Linehan, col. 9, lines 11-12. Control keys are identified by an index number. See Linehan, col. 10, lines 13-15. One control key is used for multiple files. See Linehan, col. 6, line 66 - col. 9, line 10. A new control key is generated for every N files and/or when M hours or days have elapsed. See Linehan, col. 9, lines 2-5.

When a user wishes to encrypt a file, the Personal Key Client sends an appropriate request to the Personal Key Server. See Linehan, col. 9, lines 35-41. The Personal Key Server generates a file encryption key (or uses a key supplied by the Personal Key Client) and encrypts the file encryption key with the current control key. See Linehan, col. 8, line 18; col. 9, lines 37-39; col. 8, lines 57-62. The Personal Key Server then prepares a header containing the encrypted file encryption key and the index number of the control key that was used to encrypt the file encryption key. See Linehan, col. 9, lines 37-41. The header and the unencrypted file encryption key are sent to the Personal Key Client, which uses the file encryption key to encrypt the file. The header is stored along with the encrypted file.

When a user needs to decrypt a file, the Personal Key Client sends the file header, which includes the encrypted file encryption key and the index number of the control key to the Personal Key Server. See Linehan, col. 9, lines 42-47. The Personal Key Server retrieves the appropriate control key from its database, decrypts the file encryption key, and sends the decrypted file encryption key back to the Personal Key Client. See Linehan, col. 9, lines 45-56. The Personal Key Client then decrypts the file using the file encryption key. See Linehan, col. 9, lines 57-58.

2. Linehan and Ote Cannot Be Properly Combined

Claim 1 of the present application reads as follows:

> 1. A method of controlling access to digital data in a file comprising:
> obtaining a passphrase from a user;
> generating a personal key based on the obtained passphrase;
> generating a file encryption key;
> encrypting the digital data in the file with the file encryption key to provide an encrypted file;
> encrypting the file encryption key with the personal key to provide an encrypted file encryption key;
> creating a file header containing the encrypted file encryption key; and
> associating the file header with the encrypted file (emphasis added).

Corresponding recitations are found in independent Claims 29 and 57.

In contrast to claim 1, which recites generating a personal key based on a passphrase obtained from a user, the control key taught by Linehan is a "randomly generated key" that is generated by a Personal Key Server. See Linehan, col. 8, line 67 – col. 9, line 18. The control key of Linehan is "generated by and kept entirely within the Personal Key Server." See Linehan, col. 9, lines 11-12. There is no need in the system of Linehan for the control key to be uniquely associated with a user. Thus, there is no need for the control key to be a "personal key" that is generated based on a passphrase provided by a user. In fact, for the system of Linehan to operate as described, the control keys cannot be associated with specific users.

Since the control key is randomly generated (i.e. not based on a passphrase obtained from a user) and is used and stored only within the Personal Key Server, the key may be used to encrypt the file encryption keys of an arbitrary number of files N, without regard to which user owns the files. Any number of files may file encryption keys encrypted by a single control key. The user needs only to supply the file header (which contains the appropriate control key index number along with the encrypted file encryption key) to the Personal Key Server and the Personal Key Server sends the decrypted file encryption key back to the Personal Key Client. In addition, since the control key of Linehan is not generated based on a passphrase obtained from a user, a new control key may be generated at any time.

The Official Action asserts that Ote teaches that a key may be generated using a passphrase, and that it would have been obvious to one of ordinary skill in the art to use the key generated by a passphrase from Ote in the file encryption system of Linehan. Official Action, p. 4. While Applicants acknowledge that the use of pass phrases to generate keys is known (See Specification, p. 2, lines 12-14), Applicants submit that one of ordinary skill in the art would not use a user-supplied passphrase to generate the control key of Linehan, since the purpose of having control keys in the system of Linehan is to provide a limited number of keys capable of being used to encrypt multiple file encryption keys. By definition, the control keys of Linehan are not associated with specific users. In fact, since the control keys of Linehan are identified by index numbers and are never provided outside the Personal Key Server, there is no need in the Linehan system to associate them with particular users or their passphrases. It appears that the purpose of the arrangement described in Linehan is to be able to encrypt file encryption keys for multiple users' files using a limited number of keys. See Linehan, col. 8, line 66 - col. 9, line 18; Linehan, col. 12, lines 3-19. Generating the control key from a user-supplied passphrase as suggested in the Official Action runs contrary to this purpose.

Combining Ote with Linehan would result in a system that would be incompatible with many of the advantages asserted by Linehan. For example, since the control keys in the hypothetical combined Linehan-Ote system would be based on a user-supplied passphrase, the modified system would be unable to change the control keys to new random numbers at predetermined time intervals. Thus, a skilled person would not modify the system of Linehan to encrypt a file encryption key with a personal key based on a passphrase obtained from a user. In light of the foregoing discussion, Applicants submit that independent Claims 1, 29, and 57 are patentable over Linehan and Ote for at least the reasons discussed above.

Similarly, a benefit asserted by Linehan is that since control keys are generated on a regular basis (e.g., based on the total number of files registered in the system or based on the number of days or hours elapsed) the number of control keys stored, and thus the amount of storage space required to store the keys, may be predicted or estimated in advance. See Linehan, col. 12, lines 3-12. Storing a unique control key for each file based on the identity of the user would frustrate this benefit.

In light of the foregoing discussion, Applicants submit that independent claims 1, 29, and 57 are patentable over Linehan and Otefor at least the reasons discussed above.

3. Linehan's Changed Control Keys are Not Used to Re-encrypt Files

While each of the dependent claims is patentable as depending from a patentable base claim, Applicants submit that certain of the dependent claims also are separately patentable. For example, with regard to claims 3, 31 and 59, the Official Action asserts that the control key of Linehan is changed periodically and re-encrypts file encryption keys. Official Action, p. 4. Applicants respectfully assert that this understanding is incorrect. A closer review of Linehan reveals that while the control key is changed periodically, a new control key is only used to encrypt new file encryption keys. In the enhanced system described by Linehan (which uses control keys), the Personal Key Server only stores the control keys, which are indexed by a control key index. See Linehan, col. 9, lines 19-24. File headers containing file encryption keys encrypted with the control keys are stored along with the encrypted files. See Linehan, col. 9, lines 40-41. The file headers also include control key index numbers that permit the Personal Key Server to choose the correct control key for decrypting a given file encryption key. See Linehan, col. 8, lines27-65.

It appears that file encryption keys generated before the control key is changed continue to be encrypted by the old control keys. This would be a necessary result of the fact that in the system described by Linehan, the file encryption keys are not stored in the Personal Key Server, but are stored as part of the headers on a separate disk or server. Linehan, col. 9, lines 35-41. If, as the Official Action asserts, existing file encryption keys were re-encrypted each time a control key was changed, the Personal Key Server may need to notify all Personal Key Clients of the change, request that all Personal Key Clients provide copies of all file headers containing encrypted file encryption keys, re-encrypt all file encryption keys, generate new file headers with the re-encrypted file encryption keys, and send all of the new file headers back to the Personal Key Clients. Linehan contains no such teaching. Accordingly, neither Linehan nor Ote discloses or suggests the recitations of claims 3, 31 and 59, and, therefore, Claims 3, 31, and 59 are separately patentable for at least these additional reasons.

4. Conclusion

In light of the above discussion, Applicants submit that Claims 1-7, 29-35 and 57-63 are patentable over Linehan and Ote, and that for at least the reasons discussed above, the rejection of such claims should be withdrawn.

B. Claims 11-17, 39-45 and 67-73

Claims 11-17, 39-45 and 67-73 recite various uses of an integrity key and message authentication code and that the integrity key is encrypted with the personal key. Additional dependent claims also recite that a verification value is generated by hashing the integrity key and the file encryption key. Applicants submit that these claims are patentable as depending from a patentable base claim, but also submit that these claims are separately patentable over the cited references for at least the reasons discussed below.

In rejecting Claims 11, 13, 39, 41, 67 and 69, the Official Action states that Linehan teaches including a message authentication code in the header associated with a file, and that it would be inherent to encrypt the key used to create the message authentication code for transit with the message authentication code. Official Action, p. 5. Applicants respectfully submit that it would not be inherent to encrypt the key used to create the message authentication code of Linehan, as it appears the key used to create the "message authentication check field" of Linehan is in fact the control key. ("The Personal Key Server then uses the control key to validate the message authentication check field..." Linehan, col. 9, lines 47-49.) As discussed above, the control key is stored only in the Personal Key Server's database and is not transmitted with the header. Thus, it would not be inherent to encrypt the key used to create the message authentication code in the system of Linehan as suggested by the Official Action.

With respect to claims 14, 42 and 70, the Official Action states that Linehan teaches hashing to create a header message authentication code. Official Action, p. 6. The Official Action cites col. 8, lines 62-65 of Linehan, which reads: "The entire file header is 'protected' against modification by a message authentication check field that is appended to the header and is encrypted under the same control key." Applicants fail to understand how the cited passage teaches a method of creating a message authentication code. Moreover, the cited references fail to teach or suggest encrypting a file encryption key, an integrity key and a verification value with a personal key as recited in Claims 14-17, 42-45, and 70-73.

In light of the above discussion, Applicants submit that Claims 11-17, 39-45 and 67-73 are separately patentable over the cited references for at least these additional reasons.

C. Claims 18-20, 46-48 and 74-76

Claims 18-20, 46-48 and 74-76 relate to shared access to the encrypted file by public key cryptography and incorporating into the header a version of the file encryption key that is encrypted with the public key of users authorized to access the file. Applicants submit that these claims are patentable as depending from a patentable base claim. Applicants also submit that these claims are separately patentable over the cited references for the reasons discussed in the Amendment mailed December 25, 2004. For the sake of brevity, those arguments will not be repeated. Nevertheless, Applicants submit that Claims 18-20, 46-48 and 74-76 are separately patentable over the cited references for at least these additional reasons.

D. Claims 21-28, 49-56 and 77-84

Claims 21-28, 49-56 and 77-84 include recitations analogous to those of Claims 11-20, 39-48 and 67-76. Applicants submit that these claims are patentable as depending from a patentable base claim. Applicants also submit that these claims are separately patentable over the cited references for reasons analogous to those discussed above with reference to Claims 11-20, 39-48 and 67-76.

CONCLUSION

In light of the above discussion, Applicants respectfully request reconsideration of the rejections of Claims 1-7, 11-35, 39-63 and 67-84. Applicants submit that the present application is in condition for allowance, which action is respectfully requested. If, in the opinion of the Examiner, a telephonic conference would expedite the examination of this matter, the Examiner is invited to call the undersigned attorney at (919) 854-1400.

Respectfully submitted,

David C. Hall
Registration No. 38,904

USPTO Customer No. 46589
Myers Bigel Sibley & Sajovec
Post Office Box 37428
Raleigh, North Carolina 27627
Telephone: 919/854-1400
Facsimile: 919/854-1401